УДК 004.38/519.711

Е. Ю. Данилина, А. А. Ситникова, Е. Н. Полякова
Научный руководитель: канд. пед. наук, доц. Е. Н. Полякова
Курганский государственный университет, Курган

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ КАК ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Аннотация. В данной статье рассмотрена актуальность использования различных биометрических методов идентификации пользователей, а также текущая ситуация на рынке биометрических программных интерфейсов производителей мобильных устройств.

Ключевые слова: биометрическая идентификация; мобильные устройства; отпечаток пальцев руки; распознавание голоса; распознавание геометрии лица.

В последнее время наибольшую популярность приобретает использование биометрической идентификации на мобильных телефонах.

Толчком к развитию биометрической идентификации личности послужил теракт, произошедший 11 сентября 2001 г. Тем самым повысился спрос на более надежные системы безопасности. Не являются исключениями взломы аккаунтов пользователей, особенно известных людей в мире политики или искусства.

На сегодняшний день существуют пять методов идентификации на мобильных устройствах с использованием биометрии: сканирование отпечатков пальцев, распознавание геометрии лица 2D и 3D, сетчатки глаза, голоса, по рисунку вен на запястье.

Дактилоскопия — наиболее распространенный биометрический метод идентификации личности и является на сегодняшний день наиболее разработанным. Этот метод строится на том, что каждый человек имеет уникальный папиллярный узор отпечатков пальцев, благодаря чему и возможна идентификация.

В конце 2014 г. был представлен Apple iPhone 5S, оснащенный технологией распознавания отпечатков пальцев Touch ID, который использовался для разблокировки смартфона и авторизации покупок в App Store. Затем появился новый смартфон с той же функцией — Galaxy S5. Реагируя на это, Apple предоставил доступ к системе Touch ID всем разработчикам мобильных приложений.

Основная идея Touch ID в том, чтобы сделать безопасность достаточно удобной и привлекательной для основной массы пользователей. И своей цели компания добилась.

Сканированный отпечаток сохраняется в защищенном от доступа извне микрокомпьютере. Причем ключ шифрования вычисляется во время загрузки устройства, а сами расшифрованные дактилоскопические данные хранятся только в оперативной памяти устройства и никогда не сохраняются на диск. При этом система время от времени удаляет данные отпечатков даже из оперативной памяти устройства, вынуждая пользователя авторизоваться с помощью кода блокировки.

Пожалуй, самое интересное в системе безопасности iOS — это именно вопрос о том, при каких обстоятельствах iOS удалит данные отпечатков из оперативной памяти устройства и заставит пользователя заново авторизоваться с помощью кода разблокировки условия, при которых система блокирует работу Touch ID и вынуждает авторизоваться с помощью кода блокировки при соблюдении некоторых условий, среди которых антиполицай: прошло более шести суток с момента последнего ввода кода блокировки, а само устройство не было разблокировано датчиком Touch ID в течение последних восьми часов. Он может усложнить работу правоохранительных органов. Последний пункт был введен сразу после нашумевшего процесса с террористом из Сан-Бернардино, когда на Apple оказывалось беспрецедентное давление.

Согласно постановлению суда от 16 февраля 2016 г., Apple была обязана оказать содействие правоохранительным органам в разблокировке iPhone, принадлежавшего Сайеду Фаруку. 2 декабря 2015 г. Фарук и его жена Ташфин Малик устроили стрельбу в здании центра для людей с ограниченным возможностями в Сан-Бернардино. Однако компания заявила, что не намерена этого делать, поскольку запрос правительства беспрецедентен и угрожает безопасности клиентов, что в результате разблокировки устройства по предложенной ФБР схеме конфиденциальность данных всех владельцев iPhone подвергнется риску.

Позже Министерство юстиции США отозвало иск к Apple, заявив, что власти смогли получить доступ к данным. Как сообщает Reuters, ФБР удалось извлечь данные с устройства без помощи компании.

Но если смотреть на эту ситуацию со стороны законодательства РФ, то такие данные можно было бы получить без согласия в соответствии с ч. 2 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных ч. 2 ст. 11 Федерального закона «О персональных данных», предусматривающей исключения, связанные с ре-

ализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Отпечаток пальца относится к персональным данным. В соответствии с ч. 1 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» к биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Исходя из определения, установленного Федеральным законом «О персональных данных», к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.

Следующая область биометрии делится на два направления: 2D и 3D распознавание лица:

- 2D — один из самых статистически неэффективных методов биометрии и с каждым годом все больше уступает другим биометрическим методам идентификации личности. В настоящее время он применяется в основном только в мультимодальных системах;
- 3D — данный метод имеет лучшие характеристики, чем 2D-метод, но, так же как и он, использует всего одну камеру. При занесении субъекта в базу субъект поворачивает голову, и алгоритм соединяет изображение воедино, создавая 3D-шаблон.

Метод проецирования шаблона состоит в том, что на объект (лицо) проецируется сетка. Время захвата и обработки изображения составляет 1–2 с для лучших моделей. В области распознавания 2D лица основным предметом разработки является программное обеспечение, т. к. обычные камеры отлично справляются с задачей захвата изображения лица. 3D-распознавание лица сейчас является куда более привлекательной областью для разработчиков.

Считалось, что самый надежный метод — это метод, основанный на сканировании сетчатки глаза. Считывание происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к крове-

носным сосудам на задней стенке глаза. Капиллярный рисунок сетчатки глаз различается даже у близнецов и может быть с большим успехом использован для идентификации личности. У этого метода практически не бывает ошибочного разрешения доступа. К сожалению, целый ряд трудностей возникает при использовании данного метода биометрии. Сканером тут является весьма сложная оптическая система, а человек должен значительное время не двигаться, пока наводится система. Сейчас такую технологию предлагает только японский производитель смартфонов Fujitsu. Устройство отсканирует сетчатку самостоятельно, пользователю нужно только открыть приложение и посмотреть на экран.

Распознавание голоса прочно связано с мобильными устройствами. С его помощью можно не только написать сообщение, но и определить местоположение, посмотреть баланс по своему банковскому счету и историю транзакций. Этот метод основан на акустических особенностях голоса индивидуума. Причинами внедрения этих систем являются повсеместное распространение телефонных сетей и практика встраивания микрофонов в мобильные устройства. Однако основным и определяющим недостатком этого подхода является низкая точность идентификации.

При рассмотрении этого метода возникает вопрос, как бороться против использования магнитофонных записей парольных фраз. Выход — генерация слов в произвольной последовательности, которую пользователь затем должен повторить.

Новая технология в сфере биометрии — использование рисунка вен руки человека. Инфракрасная камера делает снимки внутренней стороны руки. Специальная программа на основе полученных данных создает цифровую свертку.

Дело в том, что, являясь довольно точным, этот метод не требует дорогого оборудования и зачастую использует ту же аппаратную базу, что и оптические сканеры отпечатков пальца. Сейчас многие компании ведут разработки в данной сфере.

Комбинированное использование биометрических систем гарантирует, что во время операции или при доступе к какому-либо интернет-сервису пользователь присутствует на самом деле. Поэтому компаниям, которые разрабатывают биометрические технологии, нужно всерьез задуматься над внедрением мультимодальных биометрических платформ.

В последнее время биометрия все чаще применяется для разблокировки телефона, идентификации пользователей мобильного банкинга и подтверждения платежей. Кроме того, биометрические решения могут применяться для других финансовых услуг, например в электронных контрактах, страховании

и политике «Know your customer». Подавляющее большинство банков намерены использовать биометрические данные в ближайшем будущем.

По мере развития информационных технологий, связанных с использованием биометрических данных в телефонах, существуют правовые проблемы. Связаны данные проблемы в первую очередь с отсутствием полноценной нормативной правовой базы для широкого внедрения биометрических технологий. Заграничный и отечественный опыт внедрения биометрических технологий показал, что у них есть не только сторонники, но и яростные противники, считающие эти технологии средством построения общества тотального контроля и нарушением гражданских свобод. Противники использования биометрических и связанных с ними информационных технологий выражают обеспокоенность по поводу того, как будет использована эта информация, не будут ли нарушаться естественные права граждан на приватность и конфиденциальность.

УДК 004.58; 159.9.01

В. О. Моторина
Научный руководитель: канд. пед. наук, доц. Е. Н. Полякова
Курганский государственный университет, Курган

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ОБЕСЕПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Аннотация. В данной статье рассмотрено понятие «социальная инженерия». Информация является одним из наиболее ценных ресурсов организации и наиболее уязвимым звеном в потери ценной информации (искажении и т. д.) является человек, которым можно управлять, манипулировать. В данной работе рассмотрены методы атак социальной инженерии и меры противодействия им.

Ключевые слова: атака; метод; социальная инженерия; меры противодействия; угрозы; человеческий фактор.

Правовое обеспечение и сопровождение большинства вопросов в любой организации независимо от формы и вида организации и учреждения — важная составляющая существования и жизнедеятельности организации, начиная от поиска соискателя на вакантную должность в организации и завершая фазой увольнения сотрудника (по собственному желанию или по факту нарушения последним законодательных актов) и прекращения действия в этом случае трудового договора или контрактного договора с лицом вступившего в договорные отношения с организацией.